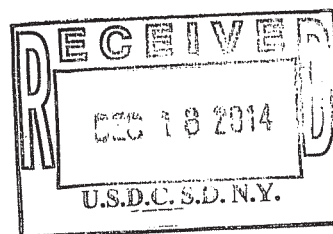


PREET BHARARA
United States Attorney for the
Southern District of New York
By: CHRISTOPHER B. HARWOOD
Assistant United States Attorney
86 Chambers Street, Third Floor
New York, New York 10007
Telephone: (212) 637-2728
Facsimile: (212) 637-2786
Email: christopher.harwood@usdoj.gov

JUDGE OETKEN

14 CV 9987



**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

-----X
THE UNITED STATES DEPARTMENT
OF THE TREASURY,

Plaintiff,

v.

THOMAS E. HAIDER,

Defendant.
-----X

Civil Case No. _____

COMPLAINT

Jury Trial Demanded

The United States Department of the Treasury (the "Government"), by its attorney, Preet Bharara, United States Attorney for the Southern District of New York, brings this action against Thomas E. Haider ("Haider" or "Defendant"), the former Chief Compliance Officer of MoneyGram International Inc. ("MoneyGram" or the "Company"), under the Currency and Foreign Transactions Reporting Act of 1970, as amended, 31 U.S.C. § 5311 *et seq.*, which is commonly referred to as the Bank Secrecy Act (the "BSA"), and its implementing regulations.

On December 18, 2014, the Financial Crimes Enforcement Network ("FinCEN"), a component of the United States Department of the Treasury, assessed a civil money penalty of \$1 million (the "assessment") against Haider. The assessment charges Haider with willfully violating the BSA and its implementing regulations. Through this action, the Government seeks

an order: (1) reducing the assessment to judgment, and awarding the Government judgment in the amount of \$1 million; and (2) enjoining Haider from participating, directly or indirectly, in the conduct of the affairs of any “financial institution” (as that term is used in the BSA and its implementing regulations) that is located in the United States or conducts business within the United States, for a term of years — to be determined at trial — sufficient to prevent future harm to the public. In support, the Government alleges as follows:

INTRODUCTION

1. Since at least 2003, MoneyGram has operated a money transfer service that enables customers to transfer money from one location to another through a global network of agents and outlets. MoneyGram outlets are independently-owned entities (such as convenience stores and internet cafes) that are authorized to transfer money through MoneyGram’s money transfer system. MoneyGram agents are the owners and/or operators of such outlets.
2. As a money transmitter, MoneyGram is subject to, and must comply with, various requirements set forth in the BSA and its implementing regulations. As relevant here — and at all times relevant to this complaint — MoneyGram was required to implement and maintain an effective anti-money laundering (“AML”) program. MoneyGram was also required to file with FinCEN suspicious activity reports (“SARs”) identifying financial transactions that: (1) were sent by or through MoneyGram; (2) involved (individually or in the aggregate) funds of at least \$2,000; and (3) MoneyGram knew, suspected, or had reason to suspect involved, among other things, the use of MoneyGram’s money transfer system to facilitate criminal activity. Such SARs were required to be filed within 30 days of MoneyGram detecting facts that may have constituted a basis for filing the SARs.

3. MoneyGram's Chief Compliance Officer was responsible for ensuring that the Company implemented and maintained an effective AML program and complied with its SAR-filing obligations. From at least 2003 through on or about May 23, 2008, Haider was MoneyGram's Chief Compliance Officer. Haider's employment at MoneyGram ended on or about May 23, 2008.

4. Notwithstanding Haider's obligations as MoneyGram's Chief Compliance Officer, at all times relevant to this complaint, Haider failed to ensure that MoneyGram (1) implemented and maintained an effective AML program and (2) fulfilled its obligation to file timely SARs. Haider's failures included the following:

- **Failure to Implement a Discipline Policy.** Haider failed to ensure that MoneyGram implemented a policy for disciplining agents and outlets that MoneyGram personnel knew or suspected were involved in fraud and/or money laundering.
- **Failure to Terminate Known High-Risk Agents/Outlets.** Haider failed to ensure that MoneyGram terminated agents and outlets that MoneyGram personnel understood were involved in fraud and/or money laundering, including outlets that Haider himself was on notice posed an unreasonable risk of fraud and/or money laundering.
- **Failure to File Timely SARs.** Haider failed to ensure that MoneyGram fulfilled its obligation to file timely SARs, including because Haider maintained MoneyGram's AML program so that the individuals responsible for filing SARs were not provided with information possessed by MoneyGram's Fraud Department that should have resulted in the filing of SARs on specific agents or outlets.
- **Failure to Conduct Effective Audits of Agents/Outlets.** Haider failed to ensure that MoneyGram conducted effective audits of agents and outlets, including outlets that MoneyGram personnel knew or suspected were involved in fraud and/or money laundering.
- **Failure to Conduct Adequate Due Diligence on Agents/Outlets.** Haider failed to ensure that MoneyGram conducted adequate due diligence on prospective agents, or existing agents seeking to open additional outlets, which resulted in, among other things, MoneyGram (1) granting outlets to agents who had previously been terminated by other money transmission companies and (2) granting additional outlets to agents who MoneyGram personnel knew or suspected were involved in fraud and/or money laundering.

5. As a result of Haider's above-described AML failures, agents and outlets that MoneyGram personnel knew or suspected were involved in fraud and/or money laundering were allowed to continue to use MoneyGram's money transfer system to facilitate their fraudulent schemes. Haider's above-referenced failures continued throughout the time period relevant to this complaint, and resulted in MoneyGram's customers suffering substantial losses (as many were duped into using MoneyGram's money transfer system to send significant sums of money to perpetrators of fraudulent schemes).

6. Under the BSA and its implementing regulations, individuals responsible for a company's failure to implement and maintain an effective AML program are liable for a civil money penalty of \$25,000 for each day that the company lacks an effective AML program. Similarly, individuals responsible for a company's failure to file required SARs are liable for a civil money penalty of no less than \$25,000 (and up to \$100,000) for each instance in which the company fails to file a required SAR. Finally, FinCEN may seek injunctive relief against such individuals to (1) enforce compliance with the BSA and its implementing regulations and (2) protect the public from future harm.

7. As a result of Haider's above-referenced AML failures — which were willful within the meaning of the civil enforcement provisions of the BSA and caused MoneyGram to violate the BSA — FinCEN has assessed a civil money penalty against him for \$1 million.

8. The Government seeks an order, pursuant to the BSA and its implementing regulations, reducing FinCEN's assessment to judgment, and awarding the Government judgment against Haider in the amount of \$1 million. The Government also seeks an order enjoining Haider from participating, directly or indirectly, in the conduct of the affairs of any

financial institution that is located in the United States or conducts business within the United States, for a term of years sufficient to prevent future harm to the public.

JURISDICTION AND VENUE

9. This Court has jurisdiction pursuant to 31 U.S.C. §§ 5320 and 5321(b)(2), as well as 28 U.S.C. §§ 1331, 1345 and 1355.

10. Venue is appropriate in this judicial district pursuant to 31 U.S.C. §§ 5320 and 5321(b)(2), and 28 U.S.C. §§ 1391(b) and 1395(a).

PARTIES

11. Plaintiff is the United States Department of the Treasury.

12. Defendant Thomas E. Haider is a former employee and officer of MoneyGram, a global money services business currently headquartered in Dallas, Texas. At all times relevant to this complaint, MoneyGram provided the public with, among other services, money transmission services. As such, MoneyGram was a “financial institution,” a “money services business” and a “money transmitter” within the meaning of the BSA and its implementing regulations. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 103.11(n)(3), (uu), *re-codified at* 31 C.F.R. § 1010.100(t)(3), (ff).¹ At all times relevant to this complaint, MoneyGram conducted significant and regular business within New York State, including through numerous agents and outlets that were located in the Southern District of New York.

13. At all times relevant to this complaint, Haider served as MoneyGram’s Chief Compliance Officer, supervising both MoneyGram’s Fraud and AML Compliance Departments. Haider’s employment with MoneyGram ended on or about May 23, 2008.

¹ Prior to 2011, the BSA regulations relevant to this complaint were codified at 31 C.F.R. Part 103. In 2011, those regulations were re-codified at 31 C.F.R. Chapter X. Because the conduct relevant to this complaint occurred prior to 2011, this complaint cites to 31 C.F.R. Part 103 with references to updated citations.

FACTS

I. BACKGROUND

A. The Relevant Statutory and Regulatory Provisions of the Bank Secrecy Act

14. As set forth below, the BSA and its implementing regulations require, among other things, that financial institutions: (1) implement an effective AML program to prevent the financial institutions from being used to facilitate money laundering or the financing of terrorist activities; and (2) report suspicious transactions involving potentially unlawful activity. *See* 31 U.S.C. § 5318(g), (h); 31 C.F.R. §§ 103.20, 103.125, *re-codified at* 31 C.F.R. §§ 1022.320, 1022.210.

15. FinCEN is a bureau within the Department of the Treasury. The Secretary of the Department of the Treasury has delegated to the Director of FinCEN the authority to implement and enforce compliance with the BSA, including through the promulgation of regulations. *See* 31 U.S.C. § 310(b)(2)(I); Treasury Order 180-01.

1. The Requirement to Implement an Effective AML Program

16. The BSA requires that all financial institutions establish an AML program that “includ[es], at a minimum”: (1) “the development of internal policies, procedures, and controls”; (2) “the designation of a compliance officer”; (3) “an ongoing employee training program”; and (4) “an independent audit function to test [the] program[.]” 31 U.S.C. § 5318(h)(1).

17. In 2002, FinCEN issued a regulation implementing 31 U.S.C. § 5318(h)(1). *See* 31 C.F.R. § 103.125. That regulation (which was in effect at all times relevant to this complaint) requires that all MSBs, including those that function as money transmitters (like MoneyGram), “develop, implement, and maintain an effective [AML] program.” *Id.* § 103.125(a). The regulation provides that “[a]n effective [AML] program is one that is reasonably designed to

prevent the [MSB] from being used to facilitate money laundering and the financing of terrorist activities,” and “shall be commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided by, the [MSB].” *Id.* § 103.125(a)-(b).

18. The above-referenced regulation, 31 C.F.R. § 103.125, also provides that an effective AML program must, “[a]t a minimum”: (1) “[i]ncorporate policies, procedures, and internal controls reasonably designed to assure compliance with [the requirements of 31 C.F.R. Part 103],” including policies for the “[f]iling [of] reports”; (2) “[d]esignate a person to assure day to day compliance with the [AML] program and [the requirements of 31 C.F.R. Part 103]” (the “AML Compliance Officer”); (3) “[p]rovide education and/or training [to] appropriate personnel concerning their responsibilities under the [AML] program, including training in the detection of suspicious transactions to the extent that the [MSB] is required to report such transactions under [31 C.F.R. Part 103]”; and (4) “[p]rovide for independent review to monitor and maintain an adequate [AML] program.” *Id.* § 103.125(d)(1)-(4).

19. Pursuant to 31 C.F.R. § 103.125, an MSB’s AML Compliance Officer must, among other things, ensure that: (1) “[t]he [MSB] properly files reports . . . in accordance with applicable requirements of [31 C.F.R. Part 103]”; (2) “[t]he [MSB’s] compliance program is updated as necessary to reflect current requirements of [31 C.F.R. Part 103], and related guidance issued by the Department of the Treasury”; and (3) “[t]he [MSB] provides appropriate training and education in accordance with [31 C.F.R. § 103.125(d)(3)].” *Id.* § 103.125(d)(2).

20. In late 2004, FinCEN issued “Interpretive Release 2004-01” (the “2004 Interpretive Release”), through which it clarified that, pursuant to 31 C.F.R. § 103.125, MSBs that do business through agents or counterparties located outside of the United States (like MoneyGram) must implement and maintain as part of their AML program risk-based policies,

procedures, and controls designed to identify and minimize money laundering and terrorist financing risks associated with such foreign agents and counterparties.

21. In the 2004 Interpretive Release, FinCEN stated that “[t]o the extent [MSBs] utilize relationships with foreign agents or counterparties to facilitate the movement of funds into or out of the United States, they must take reasonable steps to guard against the flow of illicit funds, or the flow of funds from legitimate sources to persons seeking to use those funds for illicit purposes, through such relationships.” Accordingly, FinCEN made clear that such MSBs’ AML programs should, among other things: (1) “establish procedures for conducting reasonable, risk-based due diligence on potential and existing foreign agents and counterparties to help ensure that such foreign agents and counterparties are not themselves complicit in illegal activity involving the [MSBs] products and services,” including “reasonable procedures . . . to evaluate, on an ongoing basis, the operations of those foreign agents and counterparties”; (2) “establish procedures for risk-based monitoring and review of transactions from, to, or through the United States that are conducted through foreign agents and counterparties” sufficient to “enable the [MSBs] to identify and, where appropriate, report as suspicious such occurrences as[] instances of unusual wire activity”; and (3) “[establish] procedures for responding to foreign agents or counterparties that present unreasonable risks of money laundering or the financing of terrorism,” including procedures that “provide for the implementation of corrective action on the part of the foreign agent or counterparty or for the termination of the relationship with any foreign agent or counterparty that [an MSB] determines poses an unacceptable risk of money laundering”

22. The 2004 Interpretive Release identified a number of “[r]elevant risk factors” that an MSB should consider in evaluating a foreign agent or counterparty, including “[a]ny

information known or readily available to the [MSB] about the foreign agent or counterparty's [AML] record" and "[t]he types and purpose of services to be provided to, and anticipated activity with, the foreign agent or counterparty." *See also Matter of Western Union Fin. Servs., Inc.*, No. 2003-2 (Mar. 6 2003) (indicating that MSBs that do business through agents or counterparties located within the United States are subject to similar requirements).

2. The Requirement to Report Suspicious Activity

23. The BSA also authorizes FinCEN to "require any financial institution, and any director, officer, employee, or agent of any financial institution, to report any suspicious transaction relevant to a possible violation of law or regulation." 31 U.S.C. § 5318(g)(1).

24. In 2000, FinCEN issued a regulation implementing 31 U.S.C. § 5318(g)(1). *See* 31 C.F.R. § 103.20. That regulation (which was amended in relevant part in 2003 and in effect at all times relevant to this complaint) requires that certain MSBs, including ones that function as money transmitters (like MoneyGram), report any "transaction . . . [that] is conducted or attempted by, at, or through [the MSB], involves or aggregates funds or other assets of at least \$2,000 . . . , and the [MSB] knows, suspects, or has reason to suspect":

- "[i]nvolves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity . . . as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation";
- "[i]s designed, whether through structuring or other means, to evade any requirements of [31 C.F.R. Part 103] or of any other regulations promulgated under the [BSA]";
- "[s]erves no business or apparent lawful purpose, and the reporting [MSB] knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction"; or
- "[i]nvolves use of the [MSB] to facilitate criminal activity."

Id. § 103.20(a)(1)-(2). At all times relevant to this complaint, MSBs were required to report such transactions by filing a SAR “no later than 30 calendar days after the date of the initial detection by the [MSB] of facts that may constitute a basis for filing a SAR[.]” *Id.* § 103.20(b)(3).

25. At all times relevant to this complaint, FinCEN required SARs to be filed on a standard form. That form was divided into multiple sections, with the following titles and purposes: (1) “Subject Information,” wherein the reporting party was to identify the suspected wrongdoer and indicate whether that individual or entity was the “[p]urchaser/sender” or “[p]ayee/receiver,” or had some other role in the suspicious transaction(s); (2) “Suspicious Activity Information,” wherein the reporting party was to provide specific details regarding the suspicious activity, including its date or date range; (3) “Transaction Location,” wherein the reporting party was to identify the physical location where the suspicious activity had occurred, and identify whether it was the “[s]elling location,” the “[p]aying location,” or some other location; (4) “Reporting Business” and “Contact for Assistance,” wherein the reporting party was to provide certain information about itself; and (5) “Suspicious Activity Information – Narrative,” wherein the reporting party was to provide a narrative description of the subject’s suspicious activity. *See* FinCEN Form 109; Form TD F 90-22.56.

3. Enforcement of the BSA and Its Implementing Regulations

26. Under the BSA, any domestic financial institution — or any “partner, director, officer, or employee” of any such institution — that “willfully” violates the BSA or its implementing regulations is liable “for a civil penalty of not more than the greater of the amount (not to exceed \$100,000) involved in the transaction (if any) or \$25,000.” 31 U.S.C.

§ 5321(a)(1). For violations of a financial institution’s duty to implement an effective AML